REMARKS

Claims 1-29 are presented for further examination. Claims 1, 18, 24, 27, and 29 have been amended.

In the Office Action mailed December 17, 2008, the Examiner rejected claims 1-29 under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 5,999,623 ("Bowman et al.") in view of U.S. Patent No. 7,143,294 ("Johnson").

Applicants respectfully disagree with the basis for the rejection and request reconsideration and further examination of the claims.

Amendments to Specification

Applicants have amended a typographical error in the specification so that the word "description" now properly reads "decryption." No new matter has been added.

Claim Rejections

In remarks accompanying the rejection, the Examiner attempts to map the claims to the primary reference, Bowman et al. Applicants respectfully disagree with the Examiner's assessment of Bowman et al. and its application to the claims.

Reference is made to Bowman et al.'s Figure 2, which shows a receiver 2a having therein a front end 14 with an antenna associated therewith, a back end 18, and decryption module 10.

The decryption module 10 has a pre-defined memory 8′ that has pre-stored therein a user identification (UID) value and a user-key (U-KEY) value. Also stored therein is a key generating algorithm (KG-ALGORITHM), which is mistakenly identified as the "RG ALGORITHM" in the drawings. A second memory 12 stores a subscription-key value (S-KEY), tag values (T1-Tn) and, in an alternative embodiment, decryption key values (D-KEY).

Both memories are coupled to a controller 11 that receives signals from the front end 14 and transmits signals to a decryption processing block (DPB) 16. The DPB block 16 includes a pre-stored D-ALGORITHM, which is used to generate the decryption algorithm in response to the D-KEY.

In operation, the receiver 2a of Bowman et al. initially receives the UID and U-KEY values at the front end 14. These values are compared with the UID value and U-KEY value stored in the memory 8′. If they match, the receiver 2a continues its operation. If the values do not match, further signals at the front end 14 associated with those UID and U-KEY values are ignored. In other words, the UID value and U-KEY value essentially are used to enable or disable the receiver 2a from further processing.

Once the receiver 2a is enabled, it then receives the S-KEY value and Tag Value at the front end. If the broadcast signal that follows is to be immediately decrypted, the S-KEY value is used by the KG-ALGORITHM generator to generate the D-KEY value that is then received at the DPB block 16 for generating the decryption algorithm.

On the other hand, if the broadcast signal that follows is to be decrypted at a later time, the S-KEY value and Tag Value are stored in the memory 12 and later used to generate the D-KEY value.

In contrast to the circuit employed in Bowman et al., claim 1 is directed to a semiconductor integrated circuit for use in an audio-video device that is arranged to produce audio-video signals from received encrypted broadcast signals. The circuit includes an input interface for receipt of an encrypted enable signal, an output interface for output of audio-video signals, and one or more hardware circuit portions arranged to process data in relation to the audio-video signals. Claim 1 further recites a first decryption circuit arranged to receive the encrypted enable signal and to decrypt the encrypted enable signal in accordance with a pre-stored key on the integrated circuit, thus generating the plain text message. Also on the circuit is a stored value contained in a store that is compared to the plain text message by a comparison circuit. If the plain text message and stored value match, the comparison circuit instructs the enabling circuit to generate an enabled signal to allow operation of at least one of the one or more hardware circuit portions, or to selectively restrict or deny operation thereof.

The one or more hardware circuit portions include a second decryption circuit arranged to receive a common key from a common key store in the integrated circuit and to decrypt the received encrypted broadcast signals in response to receipt of the common key and the enable signal.

One feature recited in claim 1 that is not found in the Bowman et al. device is the storing of all keys in the integrated circuit in order to avoid risk to the security of the device through tampering or interception of transmitted key values. In other words, the encrypted broadcast signals can be produced as audio-video signals without requiring receipt of one or more transmitted keys.

In Bowman et al., it is necessary for the device to receive the transmitted S-KEY value and Tag Value in order to generate the decryption algorithm and enable further processing of the received signals. In the present claimed integrated circuit, all of the keys or stored values are already present on the circuit and no reception of transmitted keys is required. This avoids possible interception of transmitted keys, whether by cable, radio, or other means.

The Johnson reference does not provide any teaching or suggestion to modify the Bowman et al. reference to provide for pre-stored keys that are not transmitted. Because Bowman et al. utilizes generation and transmission of UID and U-KEY values, S-KEY values, and Tag Values at its Broadcast Data Access Controller as well as at the receiver, there would need to be a wholesale redesign of the Bowman et al. system. Moreover, Bowman et al. is a radio frequency system that does not utilize cables, and hence the system, which is principally designed for satellite usage, would not be optimized if the receiver had to have the keys pre-stored thereon. Hence, Bowman et al. does not recognize the need to have pre-stored keys in view of its method of operation.

Applicants respectfully submit that neither Bowman et al. nor Johnson, taken alone or in any combination thereof, teach or suggest the circuit of claim 1. Dependent claims 2-17 are allowable for the features recited therein as well as for the reasons why claim 1 is allowable.

Independent claim 18 is directed to a television decoder for encrypted broadcast signals that includes a semiconductor integrated circuit along the lines of claim 1. Applicants respectfully submit that claim 18 is in condition for allowance for the reasons why claim 1 is allowable.

Independent claim 19 is directed to a method of providing an audio-video device to a user in which one or more of the hardware circuit portions of the audio-video device are

inoperable or have reduced functionality. In the method a subscription agreement is arranged with the end user after the equipment is supplied to the end user, and then an enable message in encrypted form is sent to the input interface of the device that instructs the monolithic semiconductor circuit to enable functionality of one or more of the hardware circuit portions. There is no teaching or suggestion in Bowman et al. or Johnson, taken alone or in any combination thereof, of arranging a subscription agreement with an end user for use of inoperable or reduced functionality equipment wherein an enable message in encrypted form is required to be input to the device to enable functionality of one or more hardware circuit portions of the device. Applicants respectfully submit that claim 19 and dependent claims 20-23 are allowable over the references cited and applied by the Examiner.

Circuit claim 24 and method claim 27 include similar features for receiving encrypted broadcast signals and producing audio-video signals therefrom in which pre-stored keys and values are used to enable the equipment and then decrypt the signals. As discussed above with respect to claim 1, nowhere does Bowman et al. or Johnson, taken alone or in any combination thereof, teach or suggest the circuit and method recited in claims 24 and 27. Applicants respectfully submit that these two claims and their respective dependent claims, 25, 26, 28, and 29, are allowable.

In view of the foregoing, applicants respectfully submit that all of the claims in this application are now clearly in condition for allowance. In the event the Examiner disagrees or finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact the undersigned by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:jk

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

1372313_1.DOC